Office of Government Ethics

Privacy Threshold Analysis Application

June 2020

Program Counsel Division

U.S. Office of Government Ethics (OGE)
Privacy Impact Assessment (PIA) for the
Privacy Threshold Analysis Application

Provide electronic copies of the signed PIA to OGE's Chief Information Security Officer and Privacy Officer.

Name of Project/System: Privacy Threshold Analysis Application
Office: LEAP

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Sara Nekou
Assistant Counsel
Legal, External Affairs and Performance Branch
Program Counsel Division
snekou@oge.gov
202-482-9229

2) Who is the system owner?

Diana J. Veilleux
Senior Agency Official for Privacy
Chief, Legal, External Affairs and Performance Branch
diana.veilleux@oge.gov
202-482-9203

3) Who is the system manager for this system or application?

Jennifer Matis
Privacy Officer
Legal, External Affairs and Performance Branch
Program Counsel Division
jmatis@oge.gov
202-482-9216

4) Who is the Chief Information Security Officer (CIO) who reviewed this document?

Ty Cooper
Chief Information Officer

Information Technology Division
jtcooper@oge.gov
(202) 482-9226

5) Who is the Senior Agency Official for Privacy who reviewed this document?

Diana J. Veilleux
Senior Agency Official for Privacy
Chief, Legal, External Affairs and Performance Branch
diana.veilleux@oge.gov
202-482-9203

6) Who is the Reviewing Official?

Ty Cooper
Chief Information Officer
Information Technology Division
jtcooper@oge.gov
202-482-9226

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, it contains information about OGE employees.

a. Is this information identifiable to the individual?

Yes.

b. Is the information about individual members of the public?

No.

c. Is the information about employees?

Yes.

2) What is the purpose of the system/application?

The Office of Government Ethics privacy program is using the Privacy Threshold Analysis (PTA) form to identify whether a particular system or project needs to comply with any privacy protection requirements and/or is subject to the Paperwork Reduction Act (PRA). The PTA application facilitates the completion of the PTA form and makes the process easier both for the privacy program staff and the person completing the form.

3) What legal authority authorizes the purchase or development of this system/application?

The Privacy Threshold Analysis application was developed by OGE staff to facilitate OGE's compliance with Privacy Act of 1974, 5 U.S.C. § 552a, as amended. Furthermore, OMB Circular A-130 requires agencies to take a coordinated approach to manage and maintain exceptional privacy programs.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

OGE employees.

2) What are the sources of the information in the system?

The information in the system is provided directly from OGE employees.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The information in the system is provided directly from OGE employees.

b. What federal agencies provide data for use in the system?

None.

c. What State and local agencies are providing data for use in the system?

None.

d. From what other third party sources will data be collected?

None.

e. What information will be collected from the employee and the public?

The PTA form collects information associated with development of a new system or project and/or modifying and recertifying a currently existing system or project. The only PII collected is the name and branch/division of the OGE employees completing or reviewing the form.

3) Accuracy, Timeliness, Reliability, and Completeness

a. How will data collected from sources other than OGE records be verified for accuracy?

N/A.

b. How will data be checked for completeness?

It is the OGE employees' responsibility to provide accurate and complete information. In addition, any questions about information provided on the PTA form can be resolved through contact with the submitting OGE employees.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

N/A. The data is intended for one-time use only. Once the PTA is completed the data is maintained for historical purposes only.

d. Are the data elements described in detail and documented?

No. However, the data elements are simple and self-explanatory.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No.

3) Will the new data be placed in the individual's record?

N/A.

4) Can the system make determinations about employees/the public that would not be possible without the new data?

No.

5) How will the new data be verified for relevance and accuracy?

N/A.

6) If the data is being aggregated, what controls are in place to protect the data from unauthorized access or use?

N/A.

7) If data is being aggregated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

N/A.

8) How will the data be retrieved? Does a personal identifier retrieve the data?

No personal identifiers will be used to retrieve the data. The data will be initially retrieved by a direct link to a newly submitted form. A pre-built "view" or report will allow the data to be retrieved by completion status. Future views may include:

- All PTAs, by branch/division
- PTAs complete by recertification due
- PTAs with following conditions:
    - PIA update needed
    - New PIA needed
    - SORN modification needed
    - New SORN needed
    - Modification to IC needed
    - Approval for a new PRA IC needed

The system can also create for download an Excel spreadsheet of all data. The spreadsheet will be used to analyze data according to the fields described above as potential future views. It will not be used to retrieve the information by personal identifier.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

N/A. Reports will not be produced on individuals.

10) What opportunities do individuals have to decline/refuse to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)?

Individuals do not have any opportunity to decline to provide the information. The information is required as part of OGE's work process, and therefore, providing the information is mandatory and the uses are required.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

N/A.

2) Is the data in the system covered by existing records disposition authority? If yes, what are the retention periods of data in this system?

The records are covered by GRS 4.2, Item 160. They may be destroyed three years after the associated Privacy Impact Assessment (PIA) is published or the determination that a PIA is unnecessary. Longer retention is authorized if required for business use.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Timely destruction of federal records is the responsibility of the Records Officer. The reports are temporary and will be destroyed when they are no longer needed by the agency.

4) Is the system using technologies in ways that the OGE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

5) How does the use of this technology affect public/employee privacy?

The system does not collect any information from the public, and it does not collect any sensitive information from OGE's employees. Therefore, OGE has determined that the application does not impose a significant risk to the privacy of the public or OGE employees.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

N/A.

8) What controls will be used to prevent unauthorized monitoring?

N/A.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

N/A. It is not a Privacy Act system of records.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A.

F. ACCESS TO DATA:

1) Who will have access to the data in the system?

All OGE employees will have read access to the data in the application. The data is not sensitive, and there is the potential that any OGE employee may have a business use for the data. Only authorized individuals with privacy program responsibilities have edit access to the data.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to OGE applications is governed by the Account Access Request Form (AARF) process, which authorizes the Information Technology Division (ITD) to create, modify, and disable network accounts, including providing access to specific OGE applications. AARF requests must be signed by the employee, his/her supervisor, and the Chief Information Officer before a request is approved to be implemented by ITD staff.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

All authorized OGE system users will have read access to all data in the application. See above.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Authorized users have been advised that agency policy prohibits them from unauthorized browsing of data and have been instructed not to engage in such activities.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? **If yes, were Privacy Act**

contract clauses inserted in their contracts and other regulatory measures addressed?

No contractors were involved with the design, development, or maintenance of the application.

6) Do other systems share data or have access to the data in the system? If yes, explain.

No.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

N/A.

8) Will other agencies share data or have access to the data in this system (Federal, State, or Local)?

No.

9) How will the data be used by the other agency?

N/A.

10) Who is responsible for assuring proper use of the data?

Each authorized user is responsible for assuring proper use of the data.

The Following Officials Have Approved the PIA for the Privacy Threshold Analysis Application:

1) System Manager

Initials: JM Date: 6/25/2020

Name: Jennifer Matis
Title: Privacy Officer

2) System Owner

Initials: DJV Date: 06/15/2020

Name: Diana Veilleux
Title: Chief, Legal, External Affairs and Performance Branch and Senior Agency Official for Privacy

3) Chief Information Officer

Initials: TC Date: 06/23/2020

Name: Ty Cooper
Title: Chief Information Officer

4) Senior Agency Official for Privacy

Initials: DJV Date: 06/15/2020

Name: Diana Veilleux
Title: Chief, Legal, External Affairs and Performance Branch and Senior Agency Official for Privacy